



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/528,312	03/17/2005	Markus Franke	2002P15289WOUS	2692
7590	02/29/2008			
Siemens Corporation Intellectual Property Department 170 Wood Avenue South Iselin, NJ 08830			EXAMINER HAILU, TESHOME	
			ART UNIT 2139	PAPER NUMBER
			MAIL DATE 02/29/2008	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/528,312	Applicant(s) FRANKE ET AL.
	Examiner TESHOME HAILU	Art Unit 2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If no period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 20 December 2007.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 6,8,10,12,14,16,18,20,22 and 23 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 6,8,10,12,14,16,18,20,22 and 23 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) Notice of Informal Patent Application
- 6) Other: _____

DETAILED ACTION

1. This office action is in reply to an amendment filed on December 20, 2007. Claims 6 and 18 have been amended.
2. Claims 1-5, 7, 9, 11, 13, 15, 17, 19 and 21 have been cancelled.
3. Claims 6, 8, 10, 12, 14, 16, 18, 20 and 22-23 are pending.

Response to Amendment

4. Applicant's arguments with respect to claims 6, 8, 10, 12, 14, 16, 18, 20 and 22-23 have been considered but are moot in view of the new ground(s) of rejection.
5. Applicant's arguments filed on December 20, 2007 with respect to the objection of claims 16 and 17 have been fully considered in view of the amendment to the claims and are persuasive. The objection of claims 16 and 17 has been withdrawn due to the cancellation of claim 17.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:
 - (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 6, 12, 18 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dierks et al (Dierks), US 6,948,061, and further in view of Oka, US Pub. No. 2002/0108042.

As per claim 6 Dierks discloses:

A method for generating and/or validating electronic signatures, the method comprising:
(column 5, line 19-20, "FIG. 4 details the manner in which a signature is validated using the system 10 illustrated in FIGS. 1 and 2").

Generating an asymmetrical key pair which includes a private signature key and a public validation key; (column 6, line 46-49, the secure token 12 attestation is accomplished prior to delivery to the end user in a secure domain. The secure token 12 is asked to generate a key pair comprising the token secure key 30 and a corresponding public key).

Calculating an electronic signature for an electronic document by means of the private signature key and by applying a predetermined signature function; (column 6, line 29-32 the validation engine 20 receives the authorization and enables the cryptographic engine 26 within the secure token 12 to execute the original request 112, creating a digital signature utilizing the private key).

Performing a certification of the public validation key wherein, when validating, only those signatures generated at a time prior to the certification of the public validation key are recognized as valid signature. (Column 1, line 26-28, the public key has been certified by a Certificate Authority, which has issued the certificate). Further Dierks disclosed, (column 9, line 42-44, the use of the private key corresponding to a certified public key is based on the ongoing validity of the certificate).

Dierks dose not explicitly discloses that only the signatures generated prior to the certification of the public key are recognized as valid. However, on the same field of endeavor, Oka teaches this limitation as, (page 9, paragraph 152, the certificate authority (CA) selects signature modules as requested by registration authorities (RA) and causes the selected modules to generate signatures based on the respective cryptosystems such as RSA cryptosystem and ECDSA signature algorithm before issuing a public key certificate containing the generated signatures).

Art Unit: 2139

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Dierks and include only the signatures generated prior to the certification of the public key are recognized as valid signature using the teaching of Oka. The modification would be obvious because one of ordinary skill in the art would be motivated to add only the signatures generated prior to the certification of the public key are recognized as valid signature and have a better way of validating a signature by determining the signature validity on the performance of public key certificate.

Claim 18 is rejected under the same reason set forth in rejection of claim 6:

As per claim 12 Dierks discloses:

The method according to Claim 6, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document. (Column 5, paragraph 29-35, the validation engine receives the authorization and enables the cryptographic engine within the secure token to execute the original request, creating a digital signature utilizing the private key. Once the message is signed, the certificate is appended and returned to the application. In turn the application sends the certificate onto the user). Further Dierks teaches (column 3, line 9-12, in the case where a relying party is sending a message, the relying party determines that a certificate is valid, encrypts the message, and sends it).

Claim 23 is rejected under the same reason set forth in rejection of claim 12:

8. Claims 8, 10, 14, 16, 20 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dierks (US 6,948,061), Oka (US Pub. No. 2002/0108042) and further in view of Watanabe (US Pub. No. 2002/0108041).

As per claim 8 Dierks in view of Oka discloses:

Art Unit: 2139

The method according to Claim 6, wherein, when certifying the public validation key, a reference to the electronic document is included in addition to a user identifier and the public validation key. (Column 6, line 46-53, the secure token attestation is accomplished prior to delivery to the end user in a secure domain. The secure token is asked to generate a key pair comprising the token secure key and a corresponding public key. It stores the private key secure and within the token, using it only in the token attestation process. The corresponding public key is taken and certified by a CA).

Dierks in view of Oka does not explicitly disclose that a reference to the electronic document and user identifier included in the process of certifying the public key. On the other hand, on the same field of endeavor, Watanabe teaches this limitation as, (page 1, paragraph 10, a public key certificate is issued by a certificate authority (CA) or an issuer authority (IA) in the public key cryptosystem. The public key certificate is prepared by user's submitting his ID and public key for example to a certificate authority and certificate authority's attaching its ID and validity for example and its signature to the information submitted by the user). Further Watanabe disclosed, (page 1, paragraph 11, the public key cryptosystem shown in FIG. 1 includes certificate's version number, certificate's serial number allocated by a certificate authority to a certificate's user, the algorithm and parameter of the above-mentioned RSA or ECC used for digital signature, the name of the certificate authority, certificate's validity, the name (user ID) of user of the certificate authority, and the public key and digital signature of this user").

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Dierks in view of Oka and include the electronic document reference and user identifier in the process of certifying the public key using the teaching of Watanabe. The modification would be obvious because one of ordinary skill in the art would be motivated to add the electronic document reference and user identifier in the process of certifying the public key and have a better way of certifying the public key by adding more identifiers to the process.

Claim 20 is rejected under the same reason set forth in rejection of claim 8:

As per claim 10 Dierks in view of Oka and Watanabe discloses:

The method according to Claim 8, wherein an implementation of the reference is performed by a calculation of a hash value for the electronic document. (Column 6, line 46-53, the secure token attestation is accomplished prior to delivery to the end user in a secure domain. The secure token is asked to generate a key pair comprising the token secure key and a corresponding public key. It stores the private key secure and within the token, using it only in the token attestation process. The corresponding public key is taken and certified by a CA).

Dierks in view of Oka and Watanabe does not explicitly disclose that the way of reference is performed by calculation of a hash value. On the other hand, on the same field of endeavor, Watanabe teaches this limitation as, (page 2, paragraph 12, the digital signature consists of data generated by generating a hash value on the basis of a hash function and applying the private key of the certificate authority to the generated hash value). Further Watanabe teaches the above limitation in FIG. 1. (See Fig. 1).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Dierks in view of Oka and Watanabe to include the calculation of hash value to perform a reference using the teaching of Watanabe. The modification would be obvious because one of ordinary skill in the art would be motivated to add the calculation of hash value to perform a reference and have a better way of certifying the public key by adding a hash value of the identifier to the process.

Claim 22 is rejected under the same reason set forth in rejection of claim 10:

As per claim 14 Dierks in view of Oka and Watanabe discloses:

The method according to Claim 8, wherein, following calculation of the signature and prior to its transfer to a recipient, a validation is performed by an author of the electronic document, in order to verify an action of intent which is expressed by the electronic document. (Column 5, paragraph 29-35, the validation engine receives the authorization and enables the

Art Unit: 2139

cryptographic engine within the secure token to execute the original request, creating a digital signature utilizing the private key. Once the message is signed, the certificate is appended and returned to the application. In turn the application sends the certificate onto the user). Further Dierks teaches (column 3, line 9-12, in the case where a relying party is sending a message, the relying party determines that a certificate is valid, encrypts the message, and sends it).

Claim 16 is rejected under the same reason set forth in rejection of claim 14:

Conclusion

9. The prior art made or record and not relied upon is considered pertinent to applicant's disclosure.

TITLE: System and method for graphical indicia for the certification of records, US Pub. No. 2002/0129241.

TITLE: Content distribution system and content distribution method, US Pub. No. 2003/0120611.

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Art Unit: 2139

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TESHOME HAILU whose telephone number is (571)270-3159. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m. PST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine L. Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Teshome Hailu

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139

February 21, 2007
